対称群

Joh @物理のかぎプロジェクト

2005-04-23

いくつかの記号の列を並べ替えるとき，並べ替える方法には何種類かあります．(記号の個数が有限ならば，可能な並べ替えの種類も有限です．)

例えば，３つの記号 (abc) を並べ替えると，$(acb), (bac), (bca), (cab), (cba)$ という並びが可能です．もとの (abc) と併せて，全部で 6 種類の並び方が可能だと言うことです．

このような,『並べ替えという演算操作そのもの』を元として集合をつくると，これは群になります．これを **対称群** と呼びます．

対称群

まずは，全ての並べ替えの操作を元とする集合が，群になることを確認しましょう．本当は，細かい部分をきちんと証明をすべきですが，ここは元の公理が満たされることを直感的に理解して，先に進むこととします．

1. 並び替えの方法について，この集合には全ての方法が含まれていますので，二つの並び替え操作を合成しても，結局，なにか既知の並び替えの方法に等しくなるはずです．つまり，この集合は，演算の合成に対して閉じています．
2. 結合則がなりたちます．(いくつか試して，確認してみてください．)
3. 単位元が存在します．(単位元は『順番を何にも変えない』操作です．)
4. 逆元が存在します．(元に戻すための逆の並べ替えもあるはずです．)

---

*1 京都に大将軍 (たいしょうぐん) という地名があります．美味しいお豆腐屋さんがたくさんあることで有名です．

*2 対称群のことを置換群とも呼ぶこともあります．全く同じ意味だ，と言い切っている教科書もあれば，対称群の部分群のことを置換群と呼ぶ，と書いているものもあります．正確な定義を知っている方は御一報下さい．

記号や関係する概念

簡単のため，(abc) を (bca) に並べ変える操作を，次のように括弧で表現することにします．上の段の文字が，この操作によってそれぞれ下の段の文字になるよ，という意味です．行列ではないので，混乱しないように注意してください．

$$\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$$

３つの文字列の並べ替え操作からなる対称群には，6 個の元 (群の元の個数を **位数** と呼ぶのでした) がありました．一般に，n 個の文字列の置換操作からなる群を，n **次対称群** と呼び，S_n のように書きます．一般に，n 個の文字列を並び替える仕方は，$n!$ 通りありますから，n 次対称群の位数は $n!$ だと言えます．

例えば，3 次対称群は具体的に次のように書けます．

$$S_3 = \left\{ \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}, \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} \right\}$$

また，文字列を表わすのにアルファベットではなく，数字を使うこともできます．例えば，次のような具合です．

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$$

互換

とくに，文字列の中の二つだけを入れ替えて，他の順番は変えないような並び替えを **互換** と呼びます．例えば，次の置換は，a はそのままに，b と c だけを入れ替える互換です．

$$\begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$$

簡単のため，このような互換を (bc) のように略記してしまうこともあります．また，互換を数字で (1 2) のように書くこともありますが，数字の 12 と間違えないように，数字の間を少し間をあけて書きます．

巡回置換

全部の並びを，一つずつずらすような置換を，**巡回置換** と呼びます．例えば，次の置換は４項の巡回置換です．

$$\begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}$$

*3 一般に，並べ替え操作は非可換であることも確認してみてください．

*4 対称群は，高次代数方程式の解の公式を探求する過程で，方程式の解の対称性に着目したラグランジェやルッフィーニにより見出され，ガロアによって全面的に用いられるようになった，いわば群論の出発点となった群です．群論が特に数学的対象の持つ『対称性』と重要な関わりを持つことを考えれば，ガロアの洞察力には改めて敬服せざるをえません．

全ての巡回置換だけを集めると群になりますが，これを **巡回群** と呼びます.

巡回置換も，簡単のために $(a\ b\ c\ d)$ のように略記してしまう場合があります．例えば，もし $(a\ c\ d\ b)$ と書いてあったら一つずつずらして見ていけばよく，『a を c に，c を d に，d を b に，b を a に置き換える置換』という意味です.

一般に巡回置換は互換の積として表わすことが可能で，n 項の巡回置換は高々 $n-1$ 個の互換に分解できます．また，一般の置換は，巡回置換と互換の積に分解できます.

theorem

n 次の巡回置換は，高々 n-1 個の互換の積に分解できます．

proof

証明は帰納法によります．$n=2$ の場合は，明らかに 1 個の互換，$n=3$ の巡回置換は二種類しかありませんが，$(1\ 2\ 3)=(1\ 2)(2\ 3)$, $(1\ 3\ 2)=(1\ 3)(2\ 3)$ となって，どちらも二個の互換で表わせます．一般に n 項の巡回置換が $n-1$ 個の互換の積で表わせるとします．このとき，$n+1$ 個の文字の巡回置換

$$\begin{pmatrix} a_1a_2....a_na_{n+1} \\ b_1b_2....b_nb_{n+1} \end{pmatrix}$$

を考えます．例えば a_1 に着目すると，$b_1, b_2, ..., b_n, b_{n+1}$ の中には，必ず a_1 と等しいものがあるはずです (これを b_p とします)．すると，

$$\begin{pmatrix} a_1a_2....a_na_{n+1} \\ b_1b_2....b_nb_{n+1} \end{pmatrix} = (b_1\ b_p)\begin{pmatrix} a_1a_2....a_na_{n+1} \\ a_1b_2....b_nb_{n+1} \end{pmatrix} = (b_1\ b_p)\begin{pmatrix} a_2....a_{n-1}a_n \\ b_2....b_{n-1}b_n \end{pmatrix}$$

となります．

$$\begin{pmatrix} a_2....a_{n-1}a_n \\ b_2....b_{n-1}b_n \end{pmatrix}$$

の部分は $n-1$ の互換で表わせるはずでしたので，全体として n 項の互換で表わせるはずです

■

系として，この定理は次のように書かれることもあります.

theorem

任意の置換は，巡回置換の積として表わせます．

互換は巡回置換の一種なのですから，この定理は明らかです.

練習問題１：次の関係を確認してみましょう

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix} = (1\ 5\ 3)(2\ 4) = (2\ 4)(1\ 5\ 3)$$

練習問題２：次の関係を確認してみましょう

$$(1\ 2\ 3)(2\ 4) \neq (2\ 4)(1\ 2\ 3)$$

偶置換と奇置換

対称群に関する概念で大事なものに，偶置換と奇置換というものがあります．巡回置換は全て互換の積として表わせるということでしたが，一般に対称群に含まれる任意の元は，互換の積として表わせるのです．

theorem

対称群に含まれる任意の元は，全て互換の積として表わせます．

さて，では対称群の元を互換の積として表わす表わし方ですが，これは一通りには決まりません．(ちょっと考えれば分かることですが，順番に並んでいるものを並び替えるとき，効率の良い並び替え方や，余分な並び替えを含むやり方など，色々あります．)

ところが，偶数個の互換の積として表わせるか，奇数個の互換の積として表わせるかという区別は，対称群の元そのものによって，どちらかに決まっているのです．

theorem

ある置換が偶置換か奇置換かは，生来的に決まっています．

proof

任意の互換を二乗すると，元の状態に戻ります．つまり，単位元は互換の二乗で表現でき，偶置換だということができます．さて，任意の偶置換 g が，他の表わし方 f を持つとします ($g = f$)．g には逆元がありますので，両側から掛けると $g^{-1}f = e$ となります．g^{-1} と e はそれぞれ偶置換ですので，f も偶置換のはずです．奇置換についても同様に照明できます■

対称群の元 σ が偶数個の互換の積として表わせる場合，これを **偶置換**，奇数個の互換の積として表わせる場合，これを **奇置換** と呼びます．偶置換か奇置換かは，sgn という記号を使い，偶置換の場合は 1，奇置換の場合は -1 だと定めておくと，簡単に表わせます．例えば，σ が偶置換の場合，$\mathrm{sgn}\sigma = 1$ という具合です．